State of Minnesota

THE OFFICE OF
ENTERPRISE TECHNOLOGY
STATE OF MINNESOTA
www.oet.state.mn.us

MINNESOTA STATE **STANDARD**

From the Office of Carolyn Parnell
Chief Information Officer, State of Minnesota

Version: 1.00
Approved Date: 4/22/2011
Approval: Signature on file

Enterprise Security Configuration Management Standard

Standard Statement

Government entities must maintain a configuration management process for all of their supported information systems and platforms. The process must address the following:

- Secure Baseline Configuration
- Configuration Maintenance
- Configuration Change Control
- Configuration Change Monitoring and Reporting

Reason for the Standard

Baseline, secure configurations provide defined and documented specifications to which an information system is built. Since a majority of security breaches occur because of system miss-configurations or unauthorized configuration changes these baselines are critical to ensure systems operate as intended. The baseline configuration provides information about specific setting of the information system, its components, and the logical placement within the information system architecture.

This standard specifies the requirements for the implementation of information security configuration management process control for information systems and assets in order to reduce the likelihood of a security breach due to miss-configured systems or the reintroduction of known vulnerabilities. It encompasses information systems for which government entities have administrative responsibility, including systems managed or hosted by third-parties on the agencies' behalf.

Secure Baseline Configuration Requirements

Government entities must identify, document, and apply secure baseline configurations based on risk exposure, data classification, compliance requirements, and operating environment that reduce the likelihood or potential impact of known security risks. At a minimum, the following items must be addressed:

- Define appropriate security configuration baseline levels in alignment with system criticality levels
- Remove or disable all unnecessary and unused software, services, protocols, and ports
- Restrict local user and administrative access based on the principle of least privilege
- Review all default settings for security risks

- When possible, employ automated mechanisms to maintain baseline configurations

Configuration Maintenance Requirements

Baseline configurations must be maintained to ensure security risks are not reintroduced into the environment after patching or other controls have been introduced. Configuration maintenance process must:

- Periodically update configurations to maintain the appropriate patch level
- Reapply security configurations as appropriate when information system undergoes a significant change (e.g, operating system upgrade, significant operating environment change)
- When possible, employ automated mechanisms to enforce baseline configurations

Configuration Change Control

Government entities must have a change control process to management changes to baseline configurations. The process must include:

- Security impact analyses to assess the potential risks of the changes
- Testing and approval of all security configuration changes
- Major changes to priority 1 or 2 information systems must be evaluated to determine if a reauthorization of the overall information system must be conducted

Configuration Change Monitoring and Reporting

All supported systems, platforms, and environments must maintain a 90% or better compliance to defined security configuration requirements. Government entities must have a process to monitor and report on system compliance to baseline configurations. This process must:

- Monitor system compliance to configuration baseline and report on systems that fall out of compliance
- Periodic audit of activities associated with configuration and change management to ensure change control processes are effective
- Validate configurations are in place and functioning appropriately; vulnerability scanning, manual configuration review, configuration compliance benchmark tools

Roles & Responsibilities

Office of Enterprise Technology (OET)

- Maintain this document
- Work with government entities to develop platform specific configuration guidelines
- Fulfill the Government Entity role and responsibilities for OET

Government Entity

- Ensure that third party contracts are in compliance with this standard
- Review and revise baseline configurations at least annually
- Maintain a change control process
- Periodically report configuration compliance for priority 1 and 2 systems to the enterprise security office

Related Information

Applicability and Exclusions

This standard is applicable to all government entities in the Executive Branch of state government that manage systems that handle, store, or transfer government data, as identified within the Enterprise Security Applicability Standard. It is also offered as guidance to other government entities outside the Executive Branch.

Agency Heads, Responsible Authorities, Chief Information Officers, Chief Information Security Officers, Data Practices Compliance Officials, and their designees who are responsible for responding to, management of, and reporting on security incidents must be aware of this standard

This requirements of this standard must be incorporated into agreements with third parties to ensure proper notification of information security incidents and their impact on state information assets.

Regulatory, Policy, Standards, & Guideline References

Minnesota Statutes 2007 Chapter 16E (Office of Enterprise Technology)

Minnesota Statutes, Chapter 13 (Data Practices Act)

Enterprise Information Security Operational Control Policy – Configuration and Patch Management Policy

Forms, Templates, and Procedures

Italicized terms can be found in the Enterprise Security Glossary of Terms

Compliance

Compliance with this standard is required within 2 years of the approval date of the standard.

History

Revision History – record additions as Major releases, edits/corrections as Minor

Date	Author	Description	Major #	Minor #
05/04/2011	Clifton Meier	Initial Release	1	0

Review History – periodic reviews to ensure compliance with program

Date	Reviewer	Description	Compliance

Approval History – record of approval phases

Phase	Description	Date
SME	Chris Buse Review & Approval	2/22/2011
ISC	Information Security Council Approval	3/2/2011
CIO	CIO Council Approval	4/28/2011